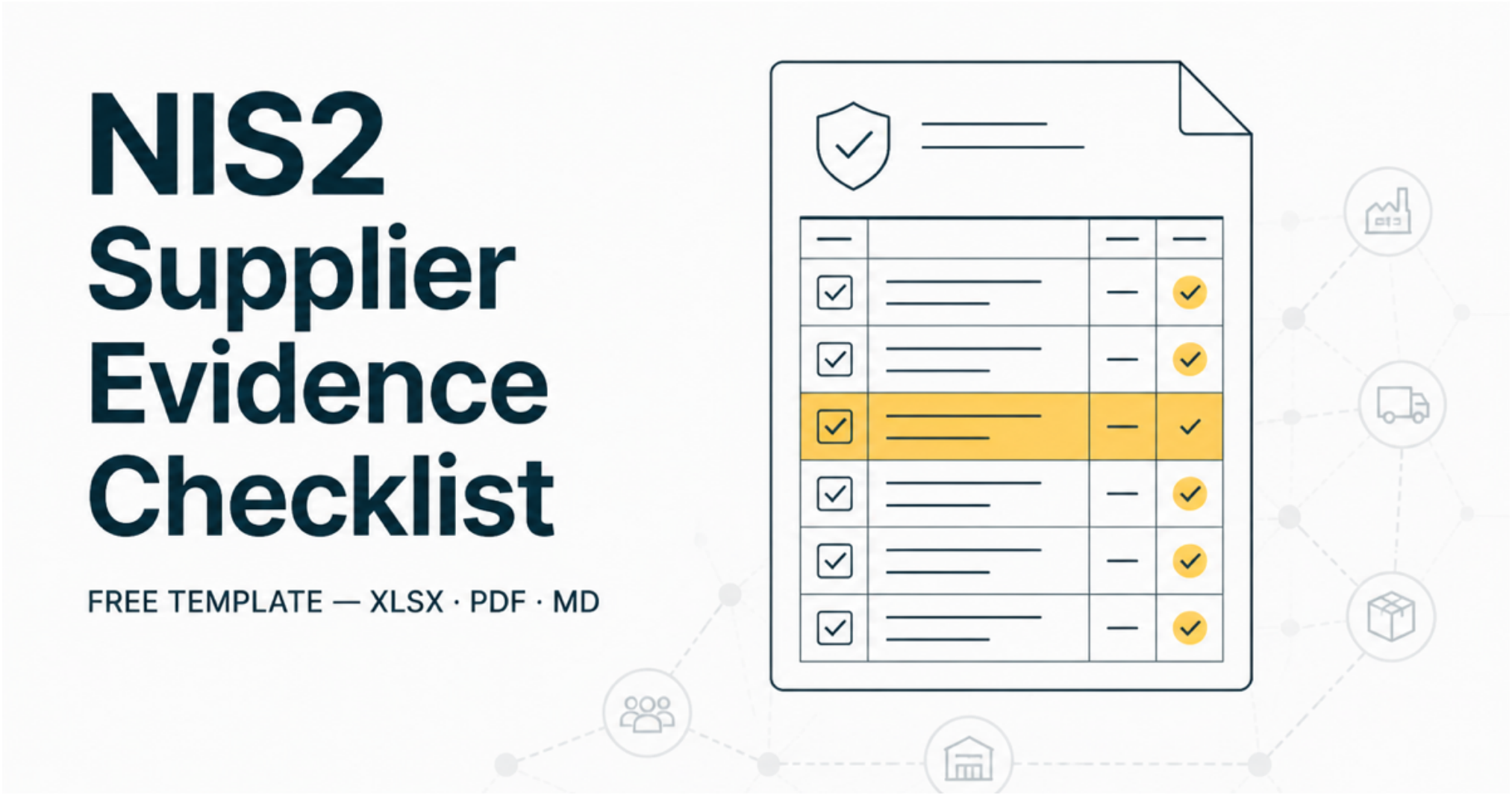

NIS2 Supplier Evidence Request Checklist

Version 1.0 · Updated 2026-07-03 · Free template · orbiqhq.com/templates/nis2-supplier-evidence-request-checklist

Supplier Register

Field reference (the XLSX carries these as columns; sample values shown from row 1):

Column	Guidance	Sample value
Supplier name		Northcloud ApS
Service provided	Describe the service you consume, not the supplier's catalogue	IaaS hosting for production platform (EU-West)
Contract ref		MSA-2024-011
Commercial owner		J. Meyer
Security reviewer		A. Kraus
Supplier security contact		security@northcloud.example
Access level	Highest applicable level	production
Data categories		Customer personal data, credentials
Countries / data location		Denmark / EU
Subcontractors disclosed		yes
Criticality tier	Score with the Criticality Rubric sheet first	T1
Last full assessment		2026-03-14
Next review due	Derived from tier cadence: T1 annual, T2 annual, T3 every 3 years / renewal	2027-03-14
Status		active
Notes		SOC 2 Type II received; next pentest summary due Q3 2026

Allowed values: **Access level**: none, network, data-readonly, data-readwrite, production · **Subcontractors disclosed**: yes, no, requested · **Criticality tier**: T1, T2, T3 · **Status**: active, onboarding, under-review, escalated, offboarding

Evidence Checklist

Field reference (the XLSX carries these as columns; sample values shown from row 1):

Column	Guidance	Sample value
Supplier name		Northcloud ApS
ID		E2
Evidence category		Certifications & independent assurance
What to request		Current certificate/attestation whose scope covers the hosted service

Column	Guidance	Sample value
Acceptable evidence types		ISO/IEC 27001 certificate with scope + expiry; SOC 2 Type II report (+ bridge letter if >12 months old); C5 where relevant
NIS2 anchor		Art. 21(3) — quality of practices
Cadence (T1 / T2 / T3)		Annual + expiry alerts / Annual / Every 3 years
Date requested		2026-02-10
Date received		2026-03-01
Status		reviewed-accepted
Reviewer		A. Kraus
Notes		ISO 27001 valid to 2027-09; scope covers EU-West region

Allowed values: **ID**: E1, E2, E3, E4, E5, E6, E7, E8, E9, E10 · **Evidence category**: Security governance / ISMS, Certifications & independent assurance, Penetration testing, Vulnerability & patch management, Secure development, Subcontractor / fourth-party disclosure, Incident notification SLA, Business continuity & disaster recovery, Access control & cryptography, Personnel security & awareness · **Status**: not-requested, requested, received, reviewed-accepted, reviewed-rejected, overdue, escalated, not-applicable

Criticality Rubric

Dimension	Question	Score 3	Score 2	Score 1
Service dependency	Would supplier failure disrupt delivery of your essential/important service?	Immediate disruption (< 24h)	Degradation within days	No material impact
Access & data	What can the supplier reach?	Production systems or sensitive/large-scale personal data	Internal systems or limited data	No system access, no meaningful data
Substitutability	How quickly could you replace the supplier?	Months+ (deep integration, few alternatives)	Weeks (alternatives exist)	Days (commodity)
Incident exposure	Would a supplier compromise plausibly trigger a NIS2 Article 23 reportable incident for you?	Yes, directly	Indirectly / uncertain	No
DECISION RULE	Total 10–12, or score 3 on BOTH Service dependency AND Incident exposure → T1. Total 7–9 → T2. Total 4–6 → T3.	T1: full evidence set (E1–E10); annual reassessment; quarterly monitoring; event-triggered re-requests	T2: core set (E1–E4, E6–E8); annual review	T3: E2 or self-attestation, E6, E7; every 3 years / renewal

Instructions

Step	Action	Where
1	Register each direct supplier and service provider: service, contract, owners, contacts, access level, data categories, subcontractor disclosure.	Supplier Register
2	Score the supplier on the four rubric dimensions and assign a tier (T1/T2/T3) using the decision rule. Re-score on any material change or incident.	Criticality Rubric
3	Create the evidence rows applicable to the tier (T1 = E1–E10; T2 = E1–E4, E6–E8; T3 = E2/attestation, E6, E7) and send the requests to the supplier security contact.	Evidence Checklist
4	Track status per row. Check certificate scope, not just existence. Reject evidence older than the cadence window and re-request with a reason.	Evidence Checklist
5	Escalate on silence: reminder at 10 business days; commercial escalation at 20; formal notice invoking the contract's audit/evidence clause at 30; documented risk decision (accept / compensate / restrict / terminate) at 45. Log every step — the trail is compliance evidence.	Evidence Checklist notes
6	Refresh on cadence (T1 annual + quarterly monitoring; T2 annual; T3 three-yearly/renewal) and on event triggers: supplier incident, subcontractor change, certificate expiry, scope change, Article 22(1) coordinated risk-assessment findings.	All sheets
7	Legal basis: Directive (EU) 2022/2555 Art. 21(2)(d) and 21(3); Implementing Regulation (EU) 2024/2690; ENISA Technical Implementation Guidance (June 2025) and Good Practices for Supply Chain Cybersecurity (June 2023). This workbook is general information, not legal advice.	—